AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method for ensuring that data generated by an untrusted entity, comprising a first computing device, and subsequently stored in a persistent storage of the untrusted entity have not been modified when the data are subsequently accessed for use by the untrusted entity, comprising steps of:

(a) the untrusted entity sending first data related information to the trusted entity for signature computation;

(b) a trusted entity, comprising a second computing device, employing a key that is only known and available for use by the trusted entity, to compute a signature for the first data related information before the data are stored in the persistent storage by the untrusted entity;

(c) the trusted entity sending the signature to the untrusted entity for storage;

(d) storing the signature and the data in the persistent storage of the untrusted entity;

(e) before the data that were stored are subsequently used by the untrusted entity, the untrusted entity sending second data related information to the trusted entity to verify that the data that were stored have not been changed;

(f) the trusted entity utilizing the key that is only known and available for use by the trusted entity to generate a temporary signature of the second data related information sent to the trusted entity;

(g) comparing the temporary signature to the stored signature; and

(h) only using the data that were stored if the step of comparing indicates that the signatures match and that the data that were stored have not been changed since the signature was computed before storing the data and the signature.

2. (Previously Presented) The method of Claim 1, wherein the first data related information is the same as the data and the second data related information is the same as the stored data.

3-4. (Canceled)

5. (Previously Presented) The method of Claim 1, wherein the first data related information comprises a digest of the data and the second data related information comprises a digest of the stored data wherein the digests are calculated by the untrusted entity based on the data and stored data.

6-7. (Canceled)

8. (Previously Presented) The method of Claim 5, wherein the first data related information further comprises:

(a) a signer identification (ID) for the untrusted entity, the signer (ID) uniquely identifying the untrusted entity and not being controlled by an operator of the untrusted entity;

9-10. (Canceled)

11. (Previously Presented) The method of Claim 1, wherein the data comprise a plurality of different sets of data, further comprising the steps of:

(a) obtaining a signer identification (ID) for the untrusted entity, the signer ID uniquely indicating the untrusted entity and not being controlled by an operator of the untrusted entity;

(b) on the trusted entity, using the key for computing an intermediate key from a concatenation of an arbitrary value and the signer ID;

(c) sending the intermediate key from the trusted entity to the untrusted entity;

(d) using the intermediate key to sign each set of the data to produce the signature for the set of data; and

(e) storing the signature, the arbitrary value, and the signer ID on the persistent storage.

12-13. (Canceled)

14. (Currently Amended) The method of Claim [[12]] 11, further comprising the step of determining if the signer ID that was received from the untrusted entity is on a list of banned signer IDs, and if so, indicating in the result that the set of data are not usable by the untrusted entity.

15-18. (Canceled)

19. (Original) A memory medium on which machine readable instructions are stored for carrying out the steps of Claim 1.

20. (Currently Amended) A untrusted entity, comprising a first gaming~~computing~~ device, in which game session related data for use by the gaming device in subsequent gaming sessions are stored, comprising:

(a) a memory in which machine instructions are stored;

(b) a persistent storage used to store data;

(c) a network interface adapted to link the untrusted entity in communication with a trusted entity, comprising a second computing device over a network; and

(d) a processor coupled to the memory, the persistent storage, and the network interface, said processor executing the machine instructions to carryout a plurality of functions, including:

(i) before storing game session related data, obtaining a signature from the trusted entity for the data determined using a key known only by a trusted entity and not available to the untrusted entity;

(ii) storing the game session related data and the signature in the persistent storage;

(iii) before using the game session related data that were stored in the persistent storage, obtaining a verification from the trusted entity that the game session related data have not been altered as a function of the signature; and

(iv) only using the game session related data that were stored if the step of obtaining the verification indicates that the game session related data that were stored have not been changed since the signature was computed by the trusted entity before storing the game session related data and the signature.

21. (Currently Amended) The untrusted entity of Claim 20, wherein the machine instructions further cause the processor to compute a digest of the game session related data before the game session related data are stored in the persistent storage, said digest being sent to a trusted entity for computing the signature.

22. (Currently Amended) The untrusted entity of Claim 21, wherein the machine instructions further cause the processor to store a signer identification (ID) that is used in computing the signature, the signer ID uniquely identifying the untrusted entity and being uncontrolled by the untrusted entity or an operator of the untrusted entity, so that the signature establishes a relationship between the game session related data before the game session related data are stored and the signer ID.

23. (Currently Amended) The untrusted entity of Claim 20, wherein the game session related data comprises a plurality of sets of game session related data, and wherein the machine instructions further cause the processor to:

(a) request an intermediate key from a trusted entity for use in computing a signature of each set of the game session related data before the set is stored in the persistent storage, the intermediate key being determined as a function of a signer identification (ID) and an arbitrary value, the signer ID uniquely identifying the untrusted entity and being uncontrolled by the untrusted entity or an operator of the untrusted entity, said untrusted entity receiving the intermediate key, the arbitrary value, and the signer ID;

(b) computing a digest of each set of the game session related data;

(c) computing the signature of the digest for each set of the game session related data using the intermediate key; and

(d) storing the signature, the arbitrary value, and the signer ID in the persistent storage.

24. (Currently Amended) The untrusted entity of Claim 23, wherein before using the game session related data that were stored, the machine instructions further cause the processor to compute a temporary digest of the game session related data that were stored; and then send the temporary digest, and the signature, the arbitrary value, and the signer ID that were stored to a trusted entity for verification that the game session related data and the signer ID have not been changed.

25-26. (Canceled)

27. (Previously Presented) A trusted entity, comprising a first computing device, that is employed in determining whether data stored in a persistent storage on an untrusted entity, comprising a second computing device, have been altered since the data were initially stored, comprising:

(a) a memory in which machine instructions are stored;

(b) a network interface adapted to link the trusted entity in communication with a untrusted entity over a network;

(c) a processor coupled to the memory, and the network interface, said processor executing the machine instructions to carryout a plurality of functions, including:

(i) employing a key that is only known and available for use by the trusted entity to compute a signature for the data before the data are stored in a persistent storage by a untrusted entity, said signature being sent to a untrusted entity and stored in a persistent storage in association with the data; and

(ii) before the data that were stored are subsequently used by a untrusted entity, utilizing the key known only to the trusted entity to compute a temporary signature for the stored data to facilitate a verification that the data that were stored have not been altered.

28. (Previously Presented) The trusted entity of Claim 27, wherein the machine instructions further cause the processor to send a result of the verification to the untrusted entity.

29. (Previously Presented) The trusted entity of Claim 27, wherein the machine instructions further cause the processor to compute the signature based upon a digest of the data that is to be stored, where the digest is received from an untrusted entity.

30. (Previously Presented) The trusted entity of Claim 27, wherein the machine instructions further cause the processor to use the key in determining the signature from a concatenation of a digest of the data that is to be stored and a signer identification (ID) uniquely identifying a untrusted entity on which the data are to be stored, wherein the signer ID is uncontrolled and unalterable by the untrusted entity and an operator of the untrusted entity, the signer ID being sent by the trusted entity to the untrusted entity with the signature.

31. (Previously Presented) The trusted entity of Claim 30, wherein the machine instructions further cause the processor to receive a temporary digest of the data that had been stored on a untrusted entity and the signer ID that had been stored on the untrusted entity, and compute a temporary signature of a concatenation of the signer ID and the temporary digest using the key, and then to verify whether the data or the signer ID that were stored were altered, by comparing the temporary signature with the signature, before sending a result of the comparison to the untrusted entity.

32. (Previously Presented) The trusted entity of Claim 27, wherein the machine instructions further cause the processor to respond to a request for an intermediate key from a untrusted entity by computing the intermediate key from an arbitrary value and a signer identification (ID) uniquely identifying the untrusted entity, wherein the signer ID is uncontrolled and unalterable by the untrusted entity and an operator of the untrusted entity, the trusted entity then sending the intermediate key, the arbitrary value, and the signer ID to the untrusted entity to enable the untrusted entity to store the arbitrary value, and the signer ill and to use the intermediate key to sign each of a plurality of sets of the data before storing the sets of the data.

33. (Previously Presented) The trusted entity of Claim 32, wherein the machine instructions further cause the processor to:

(a) receive a temporary digest of a set of data that had been stored, along with the signature, the arbitrary value, and the signer ID that were stored;

(b) compute a temporary intermediate key by using the key to sign the signer ID and the arbitrary value that were received;

(c) compute a temporary signature for the set of data using an intermediate key;

(d) compare the temporary signature and the signature to verify whether the set of data or the signer ID that have been stored have been altered; and

(e) sending a result of the comparison to the untrusted entity.

34-36. (Canceled)